WHAT IS CLAIMED IS:

1. A method for handling Link State Packets (LSPs) sent between processing nodes within a computer network, the method comprising:

at a first node, receiving an LSP sent by a second node, wherein the LSP specifies connectivity information regarding the second node;

determining whether the received LSP is an updated LSP even when the received LSP is considered older than another LSP previously sent by the second node to the first node; and

if it is determined that the received LSP is an updated LSP, performing updating procedures on LSP information that is maintained by the first node, wherein the LSP information was obtained from one or more LSPs sent by the second node.

2. A method as recited in claim 1, wherein the received LSP is in a format which complies with a link state type routing protocol and the LSP is considered older than another LSP based on one or more rules of the link state type routing protocol.

3. A method as recited in claim 2, wherein the received LSP is in a format which complies with the IS-IS Protocol and the LSP is considered older than another LSP based on one or more rules of the IS-IS protocol.

4. A method as recited in claim 1, wherein the determination of whether the received LSP is an updated LSP comprises determining that the received LSP is an updated LSP if (i) authentication succeeds for the received LSP, (ii) the LSP is considered older than

another LSP previously stored for the second node, and (iii) the stored LSP fails authentication.

5. A method as recited in claim 4, further comprising sending a second LSP from the first node back to the second node if it is determined that the received LSP is an updated LSP.

6. A method as recited in claim 5, further comprising forming the second LSP by stripping the connectivity information from the received LSP and replacing the authentication with a new authentication.

7. A method as recited in claim 6, further comprising receiving at the first node a third LSP sent from the second node in response to the second LSP, wherein the third LSP contains the updated sequence number, wherein performing the updating procedures on the LSP information is based on the received third LSP.

8. A method as recited in claim 7, further comprising updating the first node's routing tables based on the LSP information maintained by the first node after the updating procedures on the LSP information are performed.

9. A method as recited in claim 8, further comprising flooding the received third LSP from the first node to its neighbor nodes if present.

10. A method as recited in claim 1, wherein the LSP information is updated only if one or more purging conditions are met that minimize security problems.

11. A method as recited in claim 1, wherein the purging conditions comprise (i) authentication is configured in the first node, (ii) the second node is coupled directly to the

first node, (iii) adjacency has been re-established between the first and second nodes, and (iv) the second node is receiving the LSP from a same interface as was used during the re-establishment of adjacency.

12. A first apparatus operable to handle Link State Packets (LSPs) sent between processing nodes within a computer network, the apparatus comprising:

one or more processors;

one or more memory, wherein at least one of the processors and memory are adapted for:

at the first apparatus, receiving an LSP sent by a second apparatus, wherein the LSP specifies connectivity information regarding the second apparatus;

determining whether the received LSP is an updated LSP even when the received LSP is considered older than another LSP previously sent by the second apparatus to the first apparatus; and

if it is determined that the received LSP is an updated LSP, performing updating procedures on LSP information that is maintained by the first apparatus, wherein the LSP information was obtained from one or more LSPs sent by the second apparatus.

13. A first apparatus as recited in claim 12, wherein the received LSP is in a format which complies with a link state type routing protocol and the LSP is considered older than another LSP based on one or more rules of the link state type routing protocol.

14. A first apparatus as recited in claim 13, wherein the received LSP is in a format which complies with the IS-IS Protocol and the LSP is considered older than another LSP based on one or more rules of the IS-IS protocol.

15. The first apparatus as recited in claim 12, wherein the determination of whether the received LSP is an updated LSP comprises determining that the received LSP is an updated LSP if (i) authentication succeeds for the received LSP, (ii) the LSP is considered older than another LSP previously stored for the second apparatus, and (iii) the stored LSP fails authentication.

16. The first apparatus as recited in claim 15, wherein at least one of the processors and memory are further adapted for sending a second LSP with an updated sequence number from the first apparatus back to the second apparatus if it is determined that the received LSP is an updated LSP.

17. The first apparatus as recited in claim 16, wherein at least one of the processors and memory are further adapted for forming the second LSP by stripping the connectivity information from the received LSP and replacing the authentication with a newly computed authentication.

18. The first apparatus as recited in claim 17, wherein at least one of the processors and memory are further adapted for receiving at the first apparatus a third LSP sent from the second apparatus in response to the second LSP, wherein the third LSP contains the updated sequence number, wherein performing the updating procedures on the LSP information is based on the received third LSP.

19. The first apparatus as recited in claim 18, wherein at least one of the processors and memory are further adapted for updating the first apparatus's routing tables based on the LSP information maintained by the first apparatus after the updating procedures on the LSP information are performed.

20. The first apparatus as recited in claim 19, wherein at least one of the processors and memory are further adapted for flooding the received third LSP from the first apparatus to its neighbor nodes if present.

21. A computer program product for handling Link State Packets (LSPs) sent between processing nodes within a computer network,, the computer program product comprising:

at least one computer readable medium;

computer program instructions stored within the at least one computer readable product configured for:

at a first node, receiving an LSP sent by a second node, wherein the LSP specifies connectivity information regarding the second node;

determining whether the received LSP is an updated LSP even when the received LSP is considered older than another LSP previously sent by the second node to the first node; and

if it is determined that the received LSP is an updated LSP, performing updating procedures on LSP information that is maintained by the first node, wherein the LSP information was obtained from one or more LSPs sent by the second node.

22. A computer program product as recited in claim 21, wherein the received LSP is in a format which complies with a link state type routing protocol and the LSP is considered older than another LSP based on one or more rules of the link state type routing protocol.

23. A computer program product as recited in claim 22, wherein the received LSP is in a format which complies with the IS-IS Protocol and the LSP is considered older than another LSP based on one or more rules of the IS-IS protocol.

24. A computer program product as recited in claim 21, wherein the determination of whether the received LSP is an updated LSP comprises determining that the received LSP is an updated LSP if (i) authentication succeeds for the received LSP, (ii) the sequence number of the LSP is lower than another LSP previously stored for the second node, and (iii) the stored LSP fails authentication.

25. A computer program product as recited in claim 24, wherein the computer program instructions stored within the at least one computer readable product are further configured for sending a second LSP with an updated sequence number from the first node back to the second node if it is determined that the received LSP is an updated LSP.

26. A computer program product as recited in claim 25, wherein the computer program instructions stored within the at least one computer readable product are further configured for forming the second LSP by stripping the connectivity information from the received LSP and replacing the authentication value of the received LSP with a newly computed authentication value.

27. A computer program product as recited in claim 26, wherein the computer program instructions stored within the at least one computer readable product are further configured for receiving at the first node a third LSP sent from the second node in response to the second LSP, wherein the third LSP contains the updated sequence number, wherein

performing the updating procedures on the LSP information is based on the received third LSP.

28. A computer program product as recited in claim 27, wherein the computer program instructions stored within the at least one computer readable product are further configured for updating the first node's routing tables based on the LSP information maintained by the first node after the updating procedures on the LSP information are performed.

29. A computer program product as recited in claim 28, wherein the computer program instructions stored within the at least one computer readable product are further configured for flooding the received third LSP from the first node to its neighbor nodes if present.

30. A computer program product as recited in claim 21, wherein the LSP information is updated only if one or more purging conditions are met that minimize security problems.

31. A computer program product as recited in claim 21, wherein the purging conditions comprise (i) authentication is configured in the first node, (ii) the second node is coupled directly to the first node, (iii) adjacency has been re-established between the first and second nodes, and (iv) the second node is receiving the LSP from a same interface as was used during the re-establishment of adjacency.

32. A first apparatus for handling Link State Packets (LSPs) sent between processing nodes within a computer network, comprising:

means for at the first apparatus, receiving an LSP sent by a second apparatus, wherein the LSP specifies connectivity information regarding the second apparatus;

means for determining whether the received LSP is an updated LSP even when the received LSP has a lower sequence number than another LSP previously sent by the second apparatus to the first apparatus; and

means for if it is determined that the received LSP is an updated LSP, performing updating procedures on LSP information that is maintained by the first apparatus, wherein the LSP information was obtained from one or more LSPs sent by the second apparatus.

33. The first apparatus as recited in claim 32, further comprising means for sending a second LSP with an updated sequence number from the first node back to the second node if it is determined that the received LSP is an updated LSP.

34. The first apparatus as recited in claim 33, further comprising means for forming the second LSP by stripping the connectivity information from the received LSP and replacing the sequence number of the received LSP with the updated sequence number.

35. The first apparatus as recited in claim 34, further comprising means for receiving at the first node a third LSP sent from the second node in response to the second LSP, wherein the third LSP contains the updated sequence number, wherein performing the updating procedures on the LSP information is based on the received third LSP.

36. The first apparatus as recited in claim 35, further comprising means for updating the first node's routing tables based on the LSP information maintained by the first node after the updating procedures on the LSP information are performed.

37. The first apparatus as recited in claim 36, further comprising means for flooding the received third LSP from the first node to its neighbor nodes if present.

38. A method for handling Link State Packets (LSPs) sent between processing nodes within a computer network, the method comprising:

at a first node, receiving an LSP sent by a second node, wherein the LSP specifies connectivity information regarding the second node;

if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, purging LSP information regarding the second node that is being maintained by the first node; and

if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, flooding a second LSP from the first node to the first node's neighbor nodes, wherein the second LSP is structured to cause a purging of LSP information regarding the second node that is being maintained by the neighbor nodes.

39. A method as recited in claim 38, further comprising forming the second LSP by stripping the connectivity information from the first LSP.

40. A method as recited in claim 38, wherein the second node is being attacked.

41. A method as recited in claim 38, wherein the received LSP is in a format which complies with a link state type routing protocol.

42. A method as recited in claim 41, wherein the received LSP is in a format which complies with the IS-IS Protocol.

43. A method as recited in claim 38, wherein the LSP information is purged and the second LSP is flooded to the first node neighbor nodes only if one or more purging conditions are met that minimize an intruder from isolating the second node from the network.

44. A method as recited in claim 43, wherein the purging conditions comprise (i) authentication is configured in the first node, (ii) the second node is coupled directly to the first node, (iii) adjacency has been re-established between the first and second nodes, and (iv) the second node is receiving the LSP from a same interface as was used during the re-establishment of adjacency.

45. A method as recited in claim 38, further comprising updating the first node's routing tables based on the LSP information maintained by the first node after the LSP information regarding the second node has been purged.

46. A method as recited in claim 44, further comprising forming the second LSP by stripping the connectivity information from the received LSP.

47. A first apparatus operable to handle Link State Packets (LSPs) sent between processing nodes within a computer network, the apparatus comprising:

one or more processors;

one or more memory, wherein at least one of the processors and memory are adapted for:

at the first apparatus, receiving an LSP sent by a second apparatus, wherein the LSP specifies connectivity information regarding the second apparatus;

if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, purging LSP information regarding the second apparatus that is being maintained by the first apparatus; and

if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, flooding a second LSP from the first apparatus to the first apparatus' neighbor apparatus, wherein the second LSP is stuctured to cause a purging of LSP information regarding the second apparatus that is being maintained by the neighbor apparatus.

48. The first apparatus as recited in claim 47, wherein the at least one of the processors and memory are further adapted for forming the second LSP by stripping the connectivity information from the first LSP.

49. The first apparatus as recited in claim 47, wherein the second apparatus is being attacked.

50. The first apparatus as recited in claim 47, wherein the received LSP is in a format which complies with a link state type routing protocol.

51. The first apparatus as recited in claim 50, wherein the received LSP is in a format which complies with the IS-IS Protocol.

52. The first apparatus as recited in claim 47, wherein the LSP information is purged and the second LSP is flooded to the first neighbor apparatus only if one or more purging conditions are met that minimize an intruder from isolating the second apparatus from the network.

53. The first apparatus as recited in claim 52, wherein the purging conditions comprise (i) authentication is configured in the first apparatus, (ii) the second apparatus is coupled directly to the first apparatus, (iii) adjacency has been re-established between the first and second apparatus, and (iv) the second apparatus is receiving the LSP from a same interface as was used during the re-establishment of adjacency.

54. The first apparatus as recited in claim 47, wherein the at least one of the processors and memory are further adapted for updating the first apparatus' routing tables based on the LSP information maintained by the first apparatus after the LSP information regarding the second apparatus has been purged.

55. The first apparatus as recited in claim 53, wherein the at least one of the processors and memory are further adapted for forming the second LSP by stripping the connectivity information from the received LSP.

56. A computer program product for handling Link State Packets (LSPs) sent between processing nodes within a computer network, the computer program product comprising:

at least one computer readable medium;

computer program instructions stored within the at least one computer readable product configured for:

at a first node, receiving an LSP sent by a second node, wherein the LSP specifies connectivity information regarding the second node;

if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, purging LSP information regarding the second node that is being maintained by the first node; and

if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, flooding a second LSP from the first node to the first node's neighbor nodes, wherein the second LSP is structured to cause a purging of LSP information regarding the second node that is being maintained by the neighbor nodes.

57. A computer program product as recited in claim 56, wherein the computer program instructions stored within the at least one computer readable product are further configured for forming the second LSP by stripping the connectivity information from the first LSP.

58. A computer program product as recited in claim 56, wherein the second node is being attacked.

59. A computer program product as recited in claim 56, wherein the received LSP is in a format which complies with a link state type routing protocol.

60. A computer program product as recited in claim 59, wherein the received LSP is in a format which complies with the IS-IS Protocol.

61. A computer program product as recited in claim 56, wherein the LSP information is purged and the second LSP is flooded to the first node neighbor nodes only if one or more purging conditions are met that minimize an intruder from isolating the second node from the network.

62. A computer program product as recited in claim 61, wherein the purging conditions comprise (i) authentication is configured in the first node, (ii) the second node is coupled directly to the first node, (iii) adjacency has been re-established between the first and second nodes, and (iv) the second node is receiving the LSP from a same interface as was used during the re-establishment of adjacency.

63. A computer program product as recited in claim 56, wherein the computer program instructions stored within the at least one computer readable product are further configured for updating the first node's routing tables based on the LSP information maintained by the first node after the LSP information regarding the second node has been purged.

64. A computer program product as recited in claim 62, wherein the computer program instructions stored within the at least one computer readable product are further configured for forming the second LSP by stripping the connectivity information from the received LSP.

65. A first apparatus operable to handle Link State Packets (LSPs) sent between processing nodes within a computer network, the first apparatus comprising:

at the first apparatus, means for receiving an LSP sent by a second apparatus, wherein the LSP specifies connectivity information regarding the second apparatus;

means for purging LSP information regarding the second apparatus that is being maintained by the first apparatus if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node; and

means for flooding a second LSP from the first apparatus to the first apparatus' neighbor apparatus if the received LSP fails authentication and the received LSP is considered newer than a stored LSP that was last previously stored for the second node by the first node, wherein the second LSP is structured to cause a purging of LSP information regarding the second apparatus that is being maintained by the neighbor apparatus.

66. The first apparatus as recited in claim 65, wherein the LSP information is purged and the second LSP is flooded to the first neighbor apparatus only if one or more purging conditions are met that minimize an intruder from isolating the second apparatus from the network.

67. The first apparatus as recited in claim 66, wherein the purging conditions comprise (i) authentication is configured in the first apparatus, (ii) the second apparatus is coupled directly to the first apparatus, (iii) adjacency has been re-established between the first and second apparatus, and (iv) the second apparatus is receiving the LSP from a same interface as was used during the re-establishment of adjacency.

68. The first apparatus as recited in claim 65, further comprising means for updating the first apparatus' routing tables based on the LSP information maintained by the first apparatus after the LSP information regarding the second apparatus has been purged.

69. The first apparatus as recited in claim 67, further comprising means for forming the second LSP by stripping the connectivity information from the received LSP.